AN ANTI-MALVERTISING MODEL FOR UNIVERSITY STUDENTS TO INCREASE SECURITY AWARENESS

NOORLAILY IZWANA BINTI IBRAHIM

UNIVERSITI TEKNOLOGI MALAYSIA

AN ANTI-MALVERTISING MODEL FOR UNIVERSITY STUDENTS TO INCREASE SECURITY AWARENESS

NOORLAILY IZWANA BINTI IBRAHIM

A dissertation submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Advanced Informatics School
Universiti Teknologi Malaysia

JUNE 2012

Dedicated to my beloved husband and family

ACKNOWLEDGEMENT

I would like to express my highest gratitude to Allah, the Most Gracious and the Most Merciful for His blessings in completing this project. I am greatly indebted to various people especially my project supervisor, Dr Mazdak Zamani for his advice, guidance and supervision throughout this project.

Special thanks go to AP Dr Zuraini Ismail for reviewing my questionnaires and the proposed model. Besides, I would like to extend my heartfelt gratitude to other lecturers in AIS, UTM for their inputs and comments in improving my research paper.

Last but not least, million thanks to my beloved husband, Mohd Shahril b Hasim and all family members for their everlasting encouragement and continuous support throughout the completion of this project. Thank you.

ABSTRACT

Accessing the website through the Internet has introduced a new way of advertising information to the users. The term “malvertising” comes from the word malware and advertising. It is one type of attack that performs malware or scareware injection into the online advertisements. The purpose of this study is to investigate security awareness on malvertising attack among university students, propose an anti-malvertising model to improve security awareness, and to evaluate the security awareness of the proposed model. The data collection of the research starts with preliminary study in understanding the malvertising issue. Then, survey questionnaire is distributed to university students from two different local universities (UTM, Kuala Lumpur and UMP, Pahang) from two different backgrounds (IT related and non-IT related courses) to investigate current security awareness on malvertising attack. The study proposes theoretical model on anti-malvertising and the security awareness will be analyzed through the survey. The proposed model consists of protection, behavior and monitoring components, identified as independent variables and the security awareness on the anti-malvertising will is identified as the dependent variable. The study had found that more than half of the students are aware with the malvertising attack by practicing protection measures, security behavior, and security monitoring that give positive impact to the students’ security awareness. This proposed theoretical model may be beneficial for the students as a basis of reference for anti-malvertising exercise, while promoting the security awareness among university students. Besides, the theoretical model can be used as a reference for the researchers in this field as well as other security practitioners in practicing the suitable components that constitute security awareness for malvertising.

ABSTRAK

Melayari laman web melalui Internet telah memperkenalkan cara baru untuk pengiklanan maklumat kepada pengguna. Perkataan "malvertising" diadaptasi daripada perkataan "malware" dan "advertising". Ia adalah suatu jenis serangan "malware" ataupun suntikan "scareware" kepada pengiklanan dalam talian. Tujuan kajian ini dilakukan adalah untuk mengkaji tahap kesedaran keselamatan terhadap serangan "malvertising" kepada pelajar universiti, untuk mencadangkan model "anti-malvertising" bagi meningkatkan kesedaran keselamatan, dan menilai tahap kesedaran keselamatan atas cadangan model tersebut. Proses pengumpulan data dalam kajian ini bermula dengan peringkat permulaan untuk mengkaji isu-isu berkaitan "malvertising". Seterusnya, soalan kajiselidik diagihkan kepada pelajar universiti dari dua buah universiti tempatan (UTM, Kuala Lumpur and UMP, Pahang), kepada pelajar daripada jurusan berbeza (jurusan berkaitan dengan IT dan tidak berkaitan dengan IT) untuk menyiasat tahap kesedaran keselamatan semasa terhadap malvertising. Kajian ini mencadangkan teori model bagi "anti-malvertising" dan tahap kesedaran keselamatan terhadap model tersebut akan dinilai. Cadangan bagi teori model tersebut mengandungi beberapa komponen seperti kawalan, sikap, dan pemantauan yang merupakan pembolehubah tidak bersandar manakala kesedaran terhadap "anti-malvertising" telah dikenal pasti sebagai pembolehubah bersandar. Kajian ini mendapati lebih daripada separuh pelajar universiti mendapat kesedaran keselamatan terhadap serangan malvertising dengan mempraktikkan kawalan, sikap dan pemantauan yang telah memberikan impak positif kepada kesedaran keselamatan pelajar universiti. Teori model yang dicadangkan ini sangat berguna kepada pelajar universiti sebagai rujukan terhadap latihan malvertising, disamping mempromosikan kesedaran keselamatan. Selain itu, model yang dicadangkan ini boleh dijadikan rujukan kepada penyelidik dan pengamal keselamatan di dalam bidang ini untuk mempraktikkan komponen yang sesuai untuk menggalakkan kesedaran keselamatan terhadap malvertising.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

IT	-	Information technology
COTI	-	Chain of trust initiatives
UTM	-	Universiti Teknologi Malaysia
UMP	-	Universiti Malaysia Pahang

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

The emergence of Internet in the recent era has changed the way people communicate and interact with each other. Undoubtedly, it does change the human's life since the information can be retrieved within a click. People can get the information and perform various transactions easier through the Internet. However, the Internet also provides variety of attacks targeted to its own users. Today, this kind of attack is very enormous and increasing (Abdulhayoglu, M., 2009).

According to Herley, C. (2009), the computers that are connected through the Internet are persistently prone to various worms, viruses, malware, spyware, adware, rootkits, keyloggers, botnet applications and zombie. The computer can be easily compromised and become the target of exploits when connecting to the Internet if proper security measures are not being put in place. Internet users are under attack as software flourishes and growing more sophisticated from day to day, making the spotted vulnerabilities keep on increasing exponentially.

Accessing the website through the Internet has introduced a new way of advertising information to the users. Online advertisement has become one of the proficient distribution channels. In contrast, the online advertisement could offer an appropriate platform for distributing the malware to the computer. The attackers targeted plentiful computers with the existence of Internet ad networks through its

malicious banner advertisements. Malware can be infected through bypassing the human mind, which is the weakest link in an electronic security system (Abraham, S. and Smith, I. C., 2010).

The attackers have been targeting on exploiting the human mind although various protection measures have been adopted for better security. The term "malvertising" comes from the word malware (or malicious software) and advertising. Hong, J (2010) explains that malvertising is one type of attack that performs malware or scareware injection by the cybercriminals into the online advertisements. In 2009, malvertising is one of the main penetration vectors that have compromised legitimate sites such as The New York Times and Gizmodo (Cluley, G., 2010). Therefore, this research is concerned about the security issues on malvertising. However, this research will only focus on security awareness on malvertising among university students and the anti-malvertising framework to increase their security awareness.

1.2 Background of the Problem

Malware is one of the security threats among the Internet users. According to BBC (2007), from 4.5 million webpages, the researchers discovered that 450,000 webpages had scripts for installing malicious code without the knowledge of the users. The attackers are more concentrating on launching the attacks to the popular and targeted websites to dispense the malware, spyware, viruses and other security threat. For the Internet users, their first visit to the infected website can provide sufficient information to the attackers to detect any security vulnerabilities, thus pushing them to download the malware to their computers. Malicious code is infiltrated into the website through variety of ways such as advertising, web server, and widgets.

The report from Cisco (2011), revealed that an average of 135 web malware is encountered per month in 2010, while October 2010 being the highest number of encountered malware (250 per month). This shows that the malware is targeting quite a number of legitimate websites to inject its malicious code. The Internet users can be infected by clicking on an ad while visiting a popular website or search engine, which is the second most common form of malware distribution, behind search engine poisoning (The Hindustan Times, 2011). This phenomenon is also called malvertising that targeted the advertising ecosystem on the web. Based on Figure 1.1, it is reported that the probability of viewing an infected website is increasing exponentially.

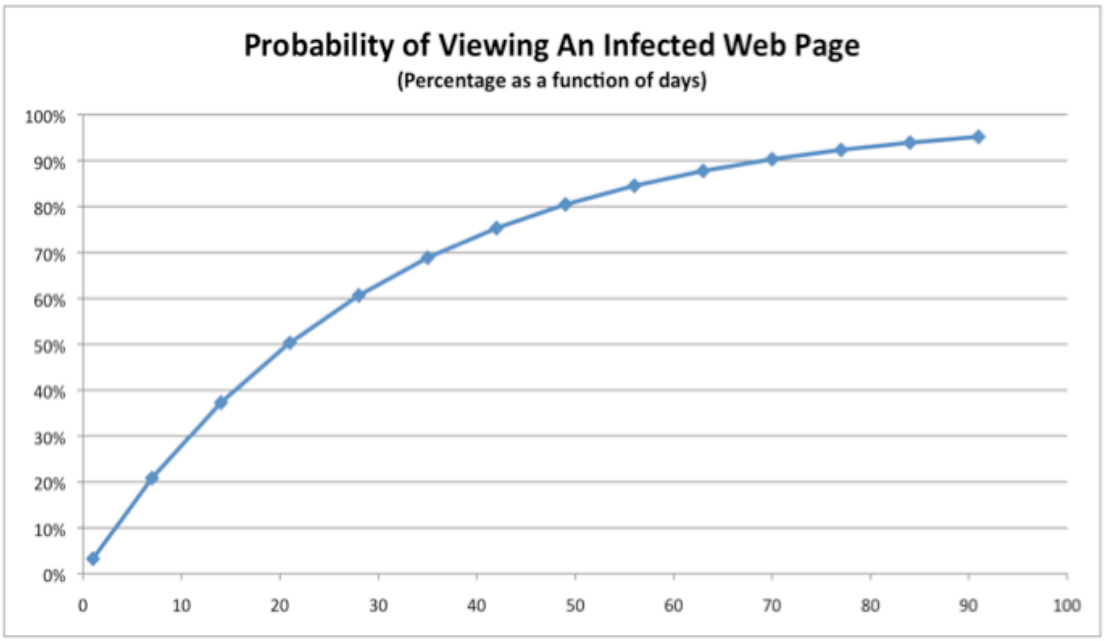

Figure 1.1: Probability of Viewing an Infected Web Page (Dasient, 2011)

The malicious banner advertisements in the website may acquire the kind of Flash programs that is very similar to normal advertisement. Nevertheless, this Flash program contains code that can attack directly to the end user's computer or redirects to the malicious site through a web browser. Many researches are carried out to the enterprise users as the companies have high risk of being infected by the malvertising.

However, there is no research had been conducted to analyze the security awareness on malvertising among the university students. Since the students also dependent on website in their routine works, they are also prone to malvertising security issues. Hence, a study on the security awareness of the students with regards to malvertising issues is needed to come out with proposed anti-malvertising framework.

1.3 Problem Statement

The extensive usage of websites has promoted malware to launch its threat to the Internet users. Vulnerabilities in the website has given a chance to the cybercriminal to hack into the website while installing malicious code, making direction to the Internet users to the fake websites which look exactly like a legitimate one. Measureable harm is very dangerous since it occurs daily due to infected advertisement on the website effects millions of users at risk.

The advertisement environment in the website is a very crucial infrastructure that supports the online services. However, the malvertisements are increasingly growing and signify a very severe security threat to the operation of the Internet. Cyber criminals are making use of greater connectivity to launch the attack to the advertisement in the website.

The running ads were being put on legitimate websites that generated rogue virus warnings, informing the end users that their computer has been compromised. As a result, the deceived Internet users from more than 60 countries bought more than one million software packages (Devine, S. M., 2010). This is because the Internet and cyber world is an unsafe place where naive users can easily become the victims to the cyber criminals (Grobler, M. *et al.,* 2011).

The duped Internet users may choose ‘Yes’ on the malicious advertising that is being prompt to download legitimate plugin. This shows that the end users with low security awareness level will be deceived by this malvertising tactic on the Internet. The current approaches in terms of information security awareness and education are descriptive and most of the researches have not explored the potential offered by motivation or behavioral theories (Mikko, T., 2000).

Figure 1.2 shows the malware infection breakdown by industry. From this figure, it is clearly shown that education industry has been the highest hit by malware in the first half of 2010 (Trend Micro, 2011). The chart clearly indicates that 44% of malware infection comes from education industry, 10% comes from technology industry, 10% also comes from the communication or media industry, 6% comes from manufacturing industry, 4% comes from healthcare industry and 4% also comes from the financial industry.

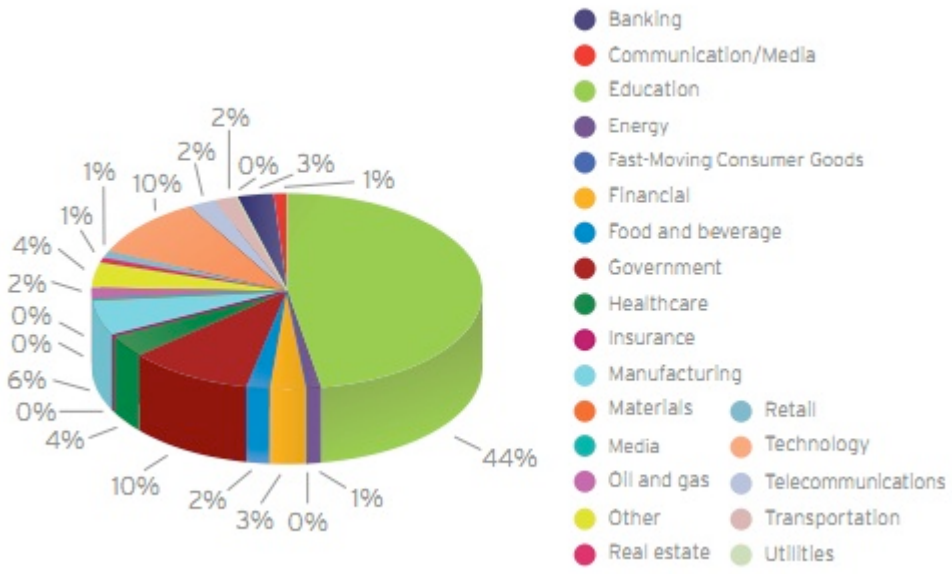

Figure 1.2: Malware Infection Breakdown by Industry (Trend Micro, 2011)

A study by Rezgui, Y. and Mark, A. (2008) reveals that conscientiousness, cultural assumptions and disbeliefs, and social conditions affect university staff behavior and attitude towards work and information security awareness. Therefore,

this research will focus more on the university students, with the following research questions:

i. What is the security awareness level of university students on the malvertising attacks?
ii. What is the proposed anti-malvertising model to improve the security awareness among university students?
iii. How is the effectiveness of the proposed anti-malvertising model?

1.4 Project Objectives

The objectives of this research are as follows:

i. To investigate security awareness among university students on malvertising attack
ii. To propose an anti-malvertising model to improve security awareness among university students
iii. To evaluate the proposed anti-malvertising model among university students

1.5 Project Aim

The aim of this research is to investigate the security awareness among university students on malvertising attack to determine their security awareness level, to propose an anti-malvertising model that can prevent students from being attacked and to evaluate the proposed anti-malvertising model.

1.6 Project Scope

The scope for this research focuses on the security awareness on malvertising and the anti-malvertising model for university students.

i. Develop and distribute questionnaires to two local universities from two different backgrounds (IT related and non-IT related students).
ii. Analyze questionnaires using statistical analysis.

1.7 Summary

This chapter aims to introduce and give overview on the proposed project, the background of the problem, problem statement, project objectives, and the project scope. The issues on students' security awareness on malvertising attacks have led to the problem statement for this project. The following chapter will look at variety of literatures and related works on malvertising.

REFERENCES

Abdulhayoglu, M. (2009). The need for a united industry in combating malware. *Computer Fraud & Security,* 5-8.

Abraham, S. and Smith, I. C. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*. Elsevier. 183-196.

Aloul, F. A. (2010). Information Security Awareness in UAE: A Survey Paper. *2010 International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE. 1-6.

Apel, M., Bockermann, C. and Meier, M. (2009). Measuring Similarity of Malware Behavior. *The 5th LCN Workshop on Security in Communications Networks (SICK 2009)*. 20-23 October. Zurich, Switzerland.

Baker, W. H. and Wallace, L. (2007). Is Information Security Under Control? Investigating Quality in Information Security Management. *IEEE Security & Privacy*. IEEE Computer Society.

BBC (2007). Google scans web pages for malware – find one in 10 infected. *Computer Fraud & Security*. 20.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2009). Effects of Individual and Organization Based Beliefs and the Moderating Role of Work Experience on Insiders' Good Security Behaviors. *2009 International Conference on Computational Science and Engineering*. IEEE Computer Society.

Cisco (2011). Cisco 4Q10, Global Threat Report, Featuring data from four core segments of Cisco Security: Intrusion Prevention System (IPS), IronPort, Remote Management Services (RMS), and ScanSafe. Retrieved on October 13, 2011, from www.cisco.com.

Cluley, G. (2010). Sizing up the malware threat – key malware trends for 2010. *Network Security,* 8-10.

Dasient (2011). The Dasient Q4 Malware Update: Significant Rise in Malvertising Attacks, Social Networking Sites Easy Dsitribution Platforms for Malware. *Dasient Smart Web Security*. Retrieved on October 14, 2011, from www.dasient.com.

De Vaus, D. A. (2001). *Research Design in Social Research* (1st edition). Great Britain: SAGE Publications Ltd.

Devine, S. M. (2010). Charges brought against scareware peddlers. *Computer Fraud & Security*. Oxford: Elsevier.

European Network and Information Security Agency (2007). Information security awareness: Local government and Internet service providers. *ENISA*.Retrieved on November 21, 2011, from www.enisa.europa.eu.

Ford, S., Cova, M., Kruegel, C. and Vigna, G. (2009). Analyzing and Detecting Malicious Flash Advertisements. *2009 Annual Computer Security Aplications Conference.* IEEE Computer Society. 363-372.

Fournier, B. J. (2010). A Broader Look at Web-based Malware: Mapping the Threat to Better Fight It. *The Chain of Trust Initiative.*

Gerber, S. B., Finn, K. V. (2005). *Using SPSS for Windows: Data Analysis and Graphics*. Springer.

Grobler, M., Jansen van Vuuren, J. and Zaaiman, J. (2011). Evaluating cyber security awareness in South Africa. *Proceedings of the 10th European Conference on Information Warfare and Security.* 7-8 July. The Institute of Cybernetics at the Tallinn University of Technology Tallinn.

Gross, B. S., Cova, M., Kruegel, C. and Vigna, G. (2011). Peering through the iFrame. *IEEE INFOCOM 2011.* IEEE. 411-415.

Harley, D. and Bureau, P. M. (2008). Drive-by Downloads from the Trenches. *2008 3rd International Conference on Malicious and Unwanted Software (MALWARE)*. IEEE. 98-103.

Hau Hsu, F., Kuo Tso, C., Chun Yeh, Y.,Jen Wang, W., and Han Chen, L. (2011). BrowserGuard: A Behavior-based Solution to Drive-by-Download Attacks. *IEEE Journal on Selected Areas in Communications.* 29(7).

Heiser, J. G. (2004). Understanding Today's Malware. *Information Security Technical Report*. 9(2): 55.

Helie, S. G. (2009). An inclusive information society needs a global approach of information security. *2009 International Conference on Availability, Reliability and Security.* IEEE Computer Society.

Herley, C. (2009). So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. *NSPW'09*. 8-11 September. Oxford, United Kingdom.

Hong, J. (2010). Malvertisements Growing as Online Security Threat. *Communications of the ACM*, 53(12): 10-11.

Kruger, H. A., Drevin, L. and Steyn, T. (2006). A Framework for Evaluating ICT Security Awareness.

Mikko, T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*. 8(1). MCB UP Ltd.

Mohamad Stambul, M. A. and Razali, R. (2011). An assessment model of information security implementation levels. *2011 International Conference on Electrical Engineering and Informatics*. 17-19 July. Bandung, Indonesia.

Online Trust Alliance (2010). Voluntary Anti-Malvertising Guidelines & Best Practices: Helping to Combat Malvertising and Preserve Trust in Interactive Advertising. *Online Trust Alliance*. Retrieved on October 5, 2011, from https://otalliance.org.

Qingguo, L. and Wei, Z. (2009). Strengthen Military Academy's Information Security Management. *2009 International Conference on Multimedia Information Networking and Security*.

Rezgui, Y. and Mark, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*. 27(7-8).

Shahzad, R. K. and Lavesson, N. (2011). Detecting Scareware by Mining Variable Length Instruction Sequences. *Information Security South Africa*.15-17 August. IEEE.1-8.

Sood, A. K. and Enbody, R. J. (2011). Malvertising – exploiting web advertising. *Computer Fraud & Security*.11-16.

Talib, S., Clarke, N. L., and Furnell, S. M. (2010). An Analysis of Information Security Awareness within Home and Work Environments. *Internanational Conference on Availability, Reliability, and Security, 2010 ARES '10*. IEEE. 196-203.

Tao, W., Shunzheng, Y, and Bailin, X. (2010). A Novel Framework for Learning to Detect Malicious Web Pages. *2010 International Forum on Information Technology and Applications.* IEEE Computer Society. 353-357.

The Hindustan Times (2011). Cyber-thieves Targeting Facebook to Spread 'Identity Detecting' Malware Infections. *The Hindustan Times*.

Trend Micro (2011). Global Threat Trends 1H 2010. *Trend Micro TrendLab*. Retrieved on December 7, 2011, from http://us.trendmicro.com.

Woodhouse, S. (2007). Information Security: End User Behavior and Corporate Culture. *Seventh International Conference on Computer and Information Technology.* IEEE Computer Society.

Xuemei, L., Yan, L. and Lixing, D. (2009). Study on Information Security of Industry Management. *2009 Asia-Pacific Conference on Information Processing.*

Yagi, T., Tanimoto, N., Hariu, T. and Itoh, M. (2010). Investigation and Analysis of Malware on Websites. *2010 12th IEEE International Symposium on Web Systems Evolution (WSE).* 17-18 September. IEEE, 73-81.

Yoshikai, N., Kurino, S., Komatsu, A., Takagi, D., Ueda, M. Inomata, A., and Numata, H. (2011). Experimental Research on Personal Awareness and Behavior for Information Security Protection. *2011 International Conference on Network-based Information Systems.* IEEE Computer Society.

Zongjiang, W. (2011). A New Type of Intelligent Network Security Model of the Campus Study. *2011 3rd International Conference on Computer Research and Development (ICCRD)*. 11-13 March. IEEE, 325 - 329.